Amendments to the Specification:

Please replace the paragraph on page 11 beginning at line 23 and ending on page 12 on line 6 with the following amended paragraph:

In order to complete the fund transfer, recipient 14 attends at Dispensing Regional Office 22 which is typically a banking institution or an affiliated agent. It should be understood that Dispensing Regional Office 22 could also be an ATM or some other interactive terminal (e.g. tourist banking kiosk) which has electronic funds transfer capability as described herein. Assuming recipient 14 is able to complete the verification ID protocol (i.e. sender 12 has communicated same to recipient 14 or recipient 14 knows the answer to a unique commonly known question etc.), then Dispensing Regional Office 22 will send a confirmation communication to Initiating Regional Office 16 in the form of a CONFIRMATION Data Packet [[94]] 96 (as shown in FIG. 2D) which includes a confirmation security ID 44. This will cause Initiating Regional Office 16 to obtain the funds (i.e. the principle funds along with any applicable international taxes, etc.) from sender 12 and to issue recipient 14 a financial card containing the predetermined amount of funds.

Please replace the paragraph on page 13 beginning at line 13 and ending on line 16 with the following amended paragraph:

FIGS. 3, 4, and 5 are flow chart diagrams ~~which~~ illustrating one embodiment of the general process steps used to accomplish transfer of funds from the sender 12 to the recipient 14 within fund transfer system 10.

The paragraph beginning at page 15 on line 21 and ending on line 30 was possibly blurred in the Examiner's copy. Please replace the paragraph with the following clearer paragraph:

Dispensing Regional Office 22 then checks to see whether recipient 14 can successfully complete the verification ID protocol provided by sender 12 (at step 152) and if not then Dispensing Regional Office 22 cancels the transfer (at step 154), notifies sender 12 and recipient 14 (at step 156), and returns (at step 158). If so, then Dispensing Regional Office 22 confirms that the fund transfer is proceeding with Initiating Regional Office 16 by sending a CONFIRMATION data packet 96 (at step 160). In response, Initiating Regional Office 16 obtains the requisite funds (i.e. the principle funds plus any applicable taxes) from sender 12 (at step 162).

Please replace the paragraph beginning on page 15 at line 31 and ending on page 16 on line 9 with the following paragraph:

Dispensing Regional Office 22 then issues a secure, anonymous, ATM compatible financial card 17 having a particular preset monetary value to recipient (at step 164) using conventionally known card issuance techniques. Finally, recipient 14 selects a unique PIN number (made up at the time of issue) for future user and security purposes (at step 166). The card is then activated and serves as a pre paid ATM compatible credit/debit transaction card for recipient 14. Once the transfer has been completed, fund transfer system 10 notifies sender 12 of the completion of the fund transfer (at step 168) and returns (at step [[164]] <u>170</u>).

Please replace the paragraph beginning on page 16 at line 10 and ending on line 23 with the following amended paragraph:

As recipient 14 uses financial card 17, fund transfer system 10 utilizes a bookkeeping functionality to keep track of usage and to deduct the appropriate amounts so that the amount of value transferred from financial card 17 does not exceed the pre-

determined amount stipulated by sender 12. Generally, financial card 17 would be issued in an "open format", but it could also be possible to issue financial card 17 in pre-set denominations. Initiating Authorization Center 18 and Dispensing Authorization Center 20 utilize the bookkeeping mechanisms that are already used by the major credit card companies. It is contemplated that fund transfer system 10 would simply be "built into" an existing credit card facility for purposes of accounting. The ~~additional~~ addition of fund transfer system 10 to an existing credit card operation would allow for the extension of fund transfers to potential clients who do not hold a credit or related bank account.

Please replace the paragraph beginning on page 19 at line 13 and ending on line 24 with the following amended paragraph:

~~Microprocessor 20~~ Microprocessor 200 is programmed to implement data processing which complies with the Federal information Processing Standards (FIPS) namely FIPS 140-1, Level 3. Microprocessor [[20]] 200 also contains a fast math coprocessor (4096-bit modules) and is programmed to implement various encryption algorithms such as DES, Triple DES and Skipjack as well as key exchange algorithms RSA, ~~Diffie-Hellman~~ Diffie-Hellman, KEA. Microprocessor [[20]] 200 also provides symmetric and asymmetric key generation on card and supports various cryptographic algorithms including RSA, DSA, DES, Triple DES, SHA-1 and MD5. The specific encryption and key generation techniques utilized by financial card 17 are selected according to the type of specific security concerns associated with implementation and operational speed requirements.

Please replace the paragraph beginning on page 20 at line 12 and ending on line 20 with the following amended paragraph:

For security reasons, the lengths of these two numbers are [[the]] equal. A modulus size of 1024 bits is considered to offer a reasonable level of security for applications like digital signatures. After further conventionally known calculations, factoring *e* and introducing *x* as plaintext and *y* as ciphertext, the formulas for encryption and decryptions are:

$y = xe \bmod m$ and

$x = yd \bmod m$, respectively.

Please replace the paragraph on page 20 beginning at line 22 and ending on page 21 on line 5 with the following amended paragraph:

In order to check signature using the public key, a rough form of "decryption" is utilized. The result of the process is not true decryption but a "hash" (i.e. where hash is generally understood as a digital algorithm or fingerprint of data which ensures authenticity) of the original data in the byte array. Since the "hash" cannot be "unhashed", the original message is hashed. If the hash of the original message matches the "decrypted" hash then the public key is associated with the private key. FIG. 7 illustrates how microprocessor 200 generates a SIGNATURE for financial card 17 using the conventionally known secure hash algorithm (SHA). A Java applet 300 hashes a DATA message 304 and then passes DATA message 304 to a card API 302 as shown. The card API 302 then encrypts the hashed DATA message using the private key along with the hashed data as shown and returns a SIGNATURE message 306 to applet 300. Applet 300 in turn provides SIGNATURE message 306.

Please replace the paragraph beginning on page 23 at line 17 and ending on line 29 with the following amended paragraph:

Further, fund transfer system 10 can be utilized within a number of different user scenarios. Examples include the student whose parents ~~which~~ wish to keep within a preset budget, the travelling executive put on a set budget by his company, the traveller who requires additional security and who wishes to pre-authorize fund transfer to himself at a destination point (i.e. destination airport), and a stranded traveller, shopper or victim of robbery of theft of personal ID. Accordingly, fund transfer system 10 provides a viable alternative to travellers cheques, credit/debit cards, and "wire" transfers, and allows any person to instantly and electronically transfer currency to any other person even in the case where neither person has a preestablished financial account with the organization, and which will still take advantage of an existing ATM network.

Please replace the paragraph beginning on page 23 at line 30 and ending on page 24 on line 7 with the following amended paragraph:

Fund transfer system 10 can specifically provide corporate users with the ability to provide financial management control for employees when travelling away from the office. Fund transfer system 10 allows a corporation to provide employees with the authority to buy and pay for goods and services remotely (i.e. by remotely issuing them cards of predetermined value) while providing direct contact with the financial computer systems at head office (i.e. transactional data could be specifically ~~send~~ sent to the corporate computer system every time a purchase using financial card 17 is made etc.)

Please replace the paragraph beginning on page 25 at line 3 and ending on line 8 with the following amended paragraph:

It should be noted that financial card 17 could be configured to be "rechargeable" for reuse purposes. It is possible that issuers could institute a recycling program for

reuse of cards whereby extra bonus points are offered when recipient 14 returns the card. Also, any odd remaining funds left on financial card 17 (i.e. low odd sums) may be converted into ~~card~~ cash by the issuer.